

## **EXHIBIT B**

**GCN****Government Computer News | GCN.com**

Thursday May 5, 2005 | Updated 5:11 PM EST May 5

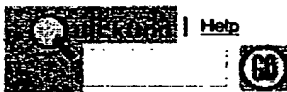
**\*Post**

Visit

Washing

[Current Issue](#) [Products Central](#) [eSeminars](#) [White Papers](#) [Events](#) [Subscribe](#) [My A](#)**Search GCN**

Advanced Search



[Biometrics](#)  
[Content Management](#)  
[Defense IT](#)  
[E-Government](#)  
[Homeland Security](#)  
[IT Infrastructure](#)  
[Mobile & Wireless](#)  
[New Products / Technology](#)  
[Outsourcing](#)  
[Policy / Regulation](#)  
[Procurement](#)  
[Section 508](#)  
[Security](#)  
[State & Local](#)  
[Storage](#)  
[Web](#)  
[Work force / Training](#)  
[Business Process \(BPM\)](#)  
[Enterprise Architecture](#)  
[Management \(Exec Center\)](#)  
[Portfolio / Program / Project](#)  
[Current Management Edition](#)

**Government Computer News****Subscribe****GCN Management****Tech Edition**

Sponsor message

October 2001; Vol. 7 No. 10a

**Don't go home without it**By Mark A. Kellner  
Special to GCN

Routers, firewalls and loading devices help telecommuters and road warriors secure both their data and computers

If you still need evidence of the importance of securing computers—both the PCs themselves and their data—you don't have to look further than the headlines from earlier this year.

In July, the FBI admitted that 13 of its 13,000 notebook PCs were stolen. At least one of them contained confidential information from a closed investigation.

Netgear Inc.'s FR314 adds firewall protection to a cable and DSL Router. It's priced at \$305.

Another 171 were missing or stolen.

The FBI might have been

embarrassed about the missing notebooks, but it is not alone. In Britain, notebook PCs have been stolen from the top-secret MI-5 and MI-6 security agencies, and the country's Ministry of Defense has reported 59 machines stolen and eight lost.

It's no laughing matter: One security manufacturer estimates that 30,000 notebook computers are stolen in U.S. airports every year. And Safeware Inc., a computer insurance agency in Columbus, Ohio, has reported 387,000 notebook PC thefts last year, up 21 percent from 1999.

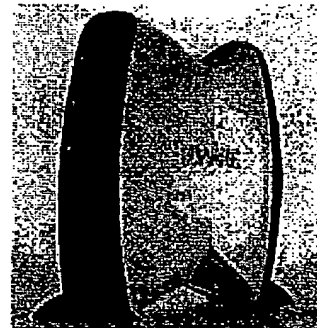
**Broadband opens a door**

On the data side, the White House's Web site, at [www.whitehouse.gov](http://www.whitehouse.gov), suffered three distributed denial-of-service attacks during May. The White House also had to defend against the Code Red worm in July and August.

The terrorist strikes last month have heightened security concerns at all levels. Such attacks thrive

**Sign for the  
FREE GCN Update****Related Tables (PDF files)**

• [Fight the threats of theft and hacker tools](#)



2Wire combi cable and its price

**The lowdown**

• How important is out-of-the-off perhaps more important than it is in After all, most federal office building measures and access controls in place more difficult, though not impossible someone's desk without authorization the road, your computer can be vulnerable to hacking if it's attached to some networks.

• Isn't broadband safe? Although providers offer various levels of security of broadband networks can create a Internet systems are essentially a lot in a neighborhood. Without safeguard

Best Available Copy

[http://www.gcn.com/state/7\\_10a/guide/16744-1.html](http://www.gcn.com/state/7_10a/guide/16744-1.html)

5/5/2005

## Whether you wear one hat



Print editions  
Regular Columnists  
E-letters

White Papers  
Forums  
Upcoming  
Previous  
News Feeds  
E-letters  
Avantoo  
Government Links  
Topic Resource Centers

GCN Events  
PostNewsweek Awards

Sponsor Reports

on the ability of hackers to reach out and touch computers—particularly those connected to broadband networks such as those using digital subscriber lines or cable Internet.

In April, Ronald Dick, director of the FBI's National Infrastructure Protection Center, told the House Energy and Commerce Committee that the threat of attacks isn't going away.

### Remote-control security

"The Department of Defense reports thousands of potential cyberattacks launched against DOD systems. GAO reports that in 1999 and 2000, the Air Force, Army and Navy recorded a combined total of 600 and 715 [serious] cyberattacks, respectively," he told the panel's oversight and investigations subcommittee.

The problems of computer security are heightened by a government push toward telecommuting. In August, Transportation Secretary Norman Mineta told a Los Angeles audience that the government is aiming to increase the number of people who work remotely.

"As a major employer, we in the federal government are increasing the number of our own employees that telework," he said. Mineta added that the fiscal 2001 Transportation Department appropriations bill requires agencies to make 25 percent of their work forces eligible for telecommuting by January and to add 25 percent each year after that until all eligible workers have the option.

Such dispersion of workers will require many to have high-speed access and appropriate computer equipment at home—but it will also leave the systems of some of those at-home workers vulnerable to theft or hacking.

Theft on the road is a perpetual concern for those who travel.

On both ends of the spectrum—data security and physical security—hardware is available to enhance protection. Although software can be used to create and maintain firewalls, having a physical firewall in place offers added security along with other advantages.

For making sure a notebook or desktop PC stays where it should, just about nothing beats a that can anchor the device to a desk or workbench.

But effective security extends beyond PCs. Telecommuters and small-office users are finding to incorporate a networking hub, either wired or wireless, so they can work in different parts.

Wired hubs generally support 10- or 100-BaseT Ethernet standards, with adapters and wiring homes, or being built into newer ones.

At the same time, the IEEE 802.11b wireless standard is gaining popularity as a networking

Many of these hubs now include firewall protection, such as Network Address Translation (NAT) and Stateful Packet Inspection, to ward off denial-of-service attacks.

### Know your networks

NAT is the translation of an IP address used within one network to a different IP address on In most cases, an organization will map local, or inside, network addresses to one or more g

office network connection, it is possible find you and spoof your computer's hardware firewall can help block suc

- Isn't a software firewall enough good line of defense, but having the that a hardware firewall provides can particularly for telecommuting feder want to assure a high level of availa network connections.

- Must-know info? The opportunit portable computer, either by error or abound. Having accessories such as cable to anchor a computer to a des detector alarm, can protect not only but also your data and work.


Printer-Friendly Version

Purchase A Report

Sponsorship Information and Advertisements

**Learn why m  
IT department:  
the future i  
Intel-based ser**

Visit [intel.com/go/gove](http://intel.com/go/gove)



intel.

Sponsorship Information and Advertisements

Best Available Copy

[http://www.gcn.com/state/7\\_10a/guide/16744-1.html](http://www.gcn.com/state/7_10a/guide/16744-1.html)

5/5/2005

[White Papers](#)  
[Product/Services Finder](#)  
[Forums](#)  
[Special Reports](#)  
[HP Blade Servers](#)  
[HP ProLiant DL135 Servers](#)  
[Custom Supplements](#)

addresses and unmap the global IP addresses on incoming packets back into local IP addresses. This approach can frustrate attempts by hackers to sniff or spoof a given IP address—one in which a distributed attack can be launched.

PAT is similar to NAT, and works when routers allow hosts on a LAN to communicate with it revealing their IP addresses.

The outbound packets have their IP address translated to a router's external IP address. Rejected at the router, which then translates them back into the private IP address of the original host for delivery.

Also known as dynamic packet filtering, Stateful Packet Inspection is a firewall architecture that operates at the network layer and examines the content of a data packet as well as its header information. It compares the packet against previous behavior on the system, along with rules set up by the administrator. These protocols can help keep hackers away, sharply reduce the possibility of distributed attacks and leverage networking capabilities to remote locations.

At the same time, the computer itself represents a security concern.

The loss or theft of a PC is, at minimum, a great inconvenience, resulting in lost time and money when replacement is found.

But in most cases, more than hardware is lost: A lot of labor can vanish in an instant. And for those with sensitive information, a lost computer can spell tremendous trouble.

#### Cable lock slot

Keeping a notebook PC secure can be aided by proper hardware add-ons.

Almost every notebook computer released in the last five years has had a small slot into which a lock can be inserted. This so-called Kensington slot, named after the company that originated and popularized the locking concept, can handle cables and even motion-sensitive alarms as part of a security system.

And the alarms are most often found on a carrying case for a PC, where they can come in handy when you're in a place where you may be distracted.

The piercing alarm emitted by the device can scare off a thief, who'd rather not be noticed.

Mark A. Kellner is a free-lance technology writer in Marina Del Rey, Calif. E-mail him at [mark@kellner2000.com](mailto:mark@kellner2000.com).

## // Marketplace

Products and services from our sponsors

### ■ **Looking for Managed Netscreen Firewall Security?**

Interland Managed Hosting Solutions include Dedicated VPNs, Enhanced Security Audits, Receive 100% uptime, 24/7 Expert Tech Support featuring Linux or Windows IBM eServer hardware replacement guaranteed.

### ■ **Security Within - Configuration based Security**

Good IT security practice requires more than anti-virus and firewall systems. Ask for our "Security Within - Configuration Based Security", which describes the reasons for a comprehensive monitoring system.

### ■ **Protect your business from spam and viruses**

Learn how VeriSign Email Security Service protects your network from spam and viruses. Buy hardware or software to install. Take advantage of the limited time Competitive Upgrade discounts up to 40%, call for details.

### ■ **Policy Management vs. Vulnerability Scanning**

Which is right for you? Vulnerability scanning products test for known vulnerabilities. Firewall products are pro-active by locking the doors in advance of a possible attack. Click to read the paper.

### ■ **Buy or Rent Used Cisco Equipment- Gov. Discount**

Buy, Rent or lease used, refurbished, Cisco Routers and Switches at great discount at our Warehouse. Thousands of satisfied customers, One-Year Warranty. GSA contract holders.

[http://www.gcn.com/state/7\\_10a/guide/16744-1.html](http://www.gcn.com/state/7_10a/guide/16744-1.html)

5/5/2005

Best Available Copy

**Buy a link NOW!**

---

[Home](#) | [About GCN](#) | [Contact GCN](#) | [Customer Help](#) | [Privacy Policy](#)  
[Careers](#) | [Editorial Info](#) | [Advertise](#) | [Link policy / Reprints](#) | [Site](#)

**GCN**

© 1996-2005 Post-Newsweek Media, Inc. All Rights Reserved.

[http://www.gcn.com/state/7\\_10a/guide/16744-1.html](http://www.gcn.com/state/7_10a/guide/16744-1.html)

5/5/2005